CyberArk
Privileged Access Manager – Digital Vault Server
v14.0

Security Target
Version 1.8
Jun 2024

Document prepared by

www.lightshipsec.com
## Document History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>08 Sept 2021</td>
<td>Marina Ibrishimova</td>
<td>First draft.</td>
</tr>
<tr>
<td>0.2</td>
<td>09 Nov 2021</td>
<td>Marina Ibrishimova</td>
<td>Updated ST to APP PP v1.4</td>
</tr>
<tr>
<td>0.3</td>
<td>19 Sep 2022</td>
<td>Marina Ibrishimova</td>
<td>Added latest TDs.</td>
</tr>
<tr>
<td>0.4</td>
<td>09 Oct 2022</td>
<td>Marina Ibrishimova</td>
<td>Addressed vendor’s comments.</td>
</tr>
<tr>
<td>0.5</td>
<td>01 Jan 2023</td>
<td>Marina Ibrishimova</td>
<td>Addressed evaluator’s comments.</td>
</tr>
<tr>
<td>0.6</td>
<td>21 Feb 2023</td>
<td>Marina Ibrishimova</td>
<td>Addressed evaluator’s comments.</td>
</tr>
<tr>
<td>0.7</td>
<td>16 Apr 2023</td>
<td>Marina Ibrishimova</td>
<td>Addressed evaluator’s comments.</td>
</tr>
<tr>
<td>0.8</td>
<td>25 Apr 2023</td>
<td>Marina Ibrishimova</td>
<td>Addressed ALC observations.</td>
</tr>
<tr>
<td>0.9</td>
<td>11 Oct 2023</td>
<td>Marina Ibrishimova</td>
<td>Added latest TDs.</td>
</tr>
<tr>
<td>1.0</td>
<td>16 Oct 2023</td>
<td>Marina Ibrishimova</td>
<td>Addressed vendor comments.</td>
</tr>
<tr>
<td>1.1</td>
<td>17 Dec 2023</td>
<td>Marina Ibrishimova</td>
<td>Addressed ASE comments.</td>
</tr>
<tr>
<td>1.2</td>
<td>24 Jan 2024</td>
<td>Enav Coresh</td>
<td>Addressed ASE comments.</td>
</tr>
<tr>
<td>1.3</td>
<td>30 Jan 2024</td>
<td>Enav Coresh</td>
<td>Addressed ASE comments.</td>
</tr>
<tr>
<td>1.4</td>
<td>11 Feb 2024</td>
<td>Enav Coresh</td>
<td>Updated product name</td>
</tr>
<tr>
<td>1.5</td>
<td>08 Apr 2024</td>
<td>Marina Ibrishimova</td>
<td>Addressed ASE comments.</td>
</tr>
<tr>
<td>1.6</td>
<td>09 May 2024</td>
<td>Marina Ibrishimova</td>
<td>Addressed ASE comments.</td>
</tr>
<tr>
<td>1.7</td>
<td>16 May 2024</td>
<td>Marina Ibrishimova</td>
<td>Addressed ASE comments.</td>
</tr>
<tr>
<td>1.8</td>
<td>13 Jun 2024</td>
<td>Marina Ibrishimova</td>
<td>Addressed ASE comments.</td>
</tr>
</tbody>
</table>
Table of Contents

1 ST Introduction ........................................................................................................... 4
  1.1 ST and TOE References ......................................................................................... 4
  1.2 TOE Overview ....................................................................................................... 4
  1.3 TOE Description ................................................................................................... 6
  1.4 Terminology .......................................................................................................... 8
2 Conformance Claims .................................................................................................. 9
3 Security Problem Definition ...................................................................................... 11
  3.1 Threats ................................................................................................................ 11
  3.2 Assumptions ......................................................................................................... 11
  3.3 Organizational Security Policies ........................................................................... 11
4 Security Objectives .................................................................................................. 12
  4.1 Objectives for the TOE ........................................................................................ 12
  4.2 Objectives for the Operational Environment ....................................................... 13
5 Security Requirements ............................................................................................... 14
  5.1 Conventions ......................................................................................................... 14
  5.2 Extended Components Definition ....................................................................... 14
  5.3 Functional Requirements .................................................................................... 14
  5.4 Assurance Requirements ..................................................................................... 22
6 TOE Summary Specification ..................................................................................... 23
  6.1 Timely Security Updates ...................................................................................... 23
  6.2 SFR Fulfilment ..................................................................................................... 23
7 Rationale ................................................................................................................... 31
  7.1 Conformance Claim Rationale .............................................................................. 31
  7.2 Security Objectives Rationale ............................................................................. 31
  7.3 Security Requirements Rationale ......................................................................... 32
8 Appendix A ................................................................................................................ 33
9 Appendix B ................................................................................................................ 66

List of Tables

Table 1: Evaluation identifiers ........................................................................................ 4
Table 2: Terminology ..................................................................................................... 8
Table 3: NIAP Technical Decisions ............................................................................. 9
Table 4: Threats ........................................................................................................... 11
Table 5: Assumptions .................................................................................................. 11
Table 6: Security Objectives ....................................................................................... 12
Table 7: Operational environment objectives .............................................................. 13
Table 8: Summary of SFRs .......................................................................................... 14
Table 9: Assurance Requirements .............................................................................. 22
Table 10: SFR Fulfilment / TOE Summary Specification ............................................ 23
Table 11: Cryptographic Algorithms ......................................................................... 29
Table 12: HMAC ........................................................................................................... 30
Table 13: Security Objectives Rationale .................................................................... 31
1 ST Introduction

1 This Security Target (ST) defines the CyberArk Privileged Access Manager – Digital Vault Server Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The CyberArk Privileged Access Manager – Digital Vault Server is the Digital Vault Server component of the CyberArk Privileged Access Manager (PAM) solution. PAM enables organizations to secure, provision, control, and monitor all activities associated with privileged identities used in enterprise systems and applications. The TOE provides secure storage and access to privileged account files, and to the administrator and session activity files.

3 The TOE operates in a Windows environment.

1.1 ST and TOE References

Table 1: Evaluation identifiers

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ST version</td>
<td>Version 1.8</td>
</tr>
<tr>
<td>ST Author</td>
<td>Lightship Security</td>
</tr>
<tr>
<td>ST Publication Date</td>
<td>Jun 13, 2024</td>
</tr>
<tr>
<td>TOE Reference</td>
<td>CyberArk Privileged Access Manager – Digital Vault Server v14.0.0.40</td>
</tr>
</tbody>
</table>

1.2 TOE Overview

1.2.1 Type

4 The TOE is an application that runs on the Windows Operating System (OS), and it is compiled with OpenSSL FIPS Object Module v1.02 and MySQL v8.0.31 database.

1.2.2 Usage

5 The TOE securely manages, stores and controls access to privileged account files, which are created by non-TOE components. The privileged account files, along with each file’s unique file key, are encrypted by Privileged Access Manager (PAM) components and sent to the TOE. For each privileged account file sent to the TOE, the TOE encrypts the unique file key, and then stores the privileged account file with its TOE-encrypted file key in a logical Safe. Each Safe has a unique key, which is used to encrypt the file key of the privileged account file stored within the Safe. The encrypted privileged account files, which are sent to and retrieved by the TOE, are never decrypted by the TOE.

6 In the evaluated configuration, the TOE runs on a hardened Windows server. The TOE’s network includes two additional servers for the other PAM components, LDAP server and a Certificate Authority (CA) server.
NOTE: The use of LDAP is optional. It is intended to be installed in the same physical network with the TOE, as part of the same environment. The TOE does not enforce any algorithms listed in the ST for the LDAP connection and is not responsible for the validation of the TLS parameters with LDAP.

Communication between the TOE and non-TOE PAM components happens over TLS as shown in Figure 1.

![Figure 1: Example TOE deployment](image)

1.2.3 Security Functions

The TOE provides the following security functions:

a) **Cryptographic Support.** The TOE implements the OpenSSL FIPS Object Module with the CyberArk libraries to provide the following cryptographic services: encryption and decryption, hashing, digital signature generation and verification, and key generation.

b) **User Data Protection.** The TOE encrypts all sensitive data stored in non-volatile memory. The TOE limits its access to network connectivity when accessing the platform’s hardware resources.

c) **Identification and Authentication.** The TOE uses X.509v3 certificates for TLS communications. The certificates are presented by the by the TOE during the TLS handshake is established. The vault certificates are authenticated by the connecting client, i.e. the Windows server PAM components, and the Linux server PAM components. The certificates can include (per generation) a CRL distribution point (CDP) to enable the clients to use a certificate revocation list (CRL) mechanisms to verify the certificate.

d) **Security Management.** The TOE provides a set of commands for administrators to manage the security functions, configuration, and other features of the TOE and OE components. A TOE administrator manages the TOE from the Password Vault Web Access (PVWA) on the Windows server in
the OE. There is no access to TOE functionality until passwords are created for the built-in Administrator user.

e) **Privacy.** The TOE does not store or transmit any Personally Identifiable Identification (PII).

f) **Protection of the TSF.** The TOE leverages anti-exploitation capabilities provided by the OS. The TOE provides integrity for installation and software updates.

g) **Trusted Path.** The TOE provides a trusted path between itself and the Privileged Session Manager (PSM), Central Policy Manager (CPM), PVWA, Privileged Session Manager SSH (Secure Shell), and Proxy (PSMP) PAM components. All communications between the TOE and these components are encrypted and authenticated over TLS v1.2 (port 443) sessions.

### 1.2.4 Non-TOE Components

The TOE operates with the following non-TOE components in the environment, which are intended to be deployed in a physically secure environment:

a) PAM Windows components, OS Microsoft Windows Server 2019, is composed of the PAM components:

i) The Privileged Session Manager (PSM) v14.0.0.9,
   
   PSM is the part of PAM that enables organizations to secure, control, and monitor privileged access to network devices over RDP connections.

ii) Password Vault Web Access (PVWA) v14.0.0.32,
   
   PVWA is the web interface of PAM that provides a single console for requesting, accessing, and managing privileged passwords throughout the environment.

iii) Central Policy Manager (CPM) v14.0.0.9,
   
   CPM automatically enforces enterprise policies for password management.

b) PAM Linux components which run on RHEL 8:

i) Privileged Session Manager SSH (Secure Shell) Proxy (PSMP) v14.0.0.14

b) LDAP Server (optional), Windows Server 2019, a central authentication server for organizations, build to provide access to internal servers for each organization user.

d) CA Server, Windows Server 2019, provides the functionality of downloading CRLs over HTTP.

e) Vault Windows Server 2019, the server on which the TOE runs.

### 1.3 TOE Description

#### 1.3.1 Physical Scope

The physical scope of the TOE is the Privileged Access Manager – Digital Vault Server Windows application. The TOE version is v14.0.0.40 and the TOE is delivered through CyberArk’s online customer portal, which uses AWS Marketplace.
The TOE delivery format is *.exe. The customer portal can be accessed after customers register to the portal https://cyberark.my.site.com/s/login.

1.3.1.1 Guidance Parts

The TOE includes the following guidance documents, which are delivered to customers through a download link that becomes available to them after they purchase the TOE and sign in for the CyberArk Privileged Access Manager - Self-Hosted customer portal:

a) Privileged Access Manager – Digital Vault Server Common Criteria Guide, v1.6 (PDF), May 2024
b) PAM Self-Hosted v14.0, 25-Jan-2024, No. A8474D5E4B6532ED3402D38B46F7DB15F650CA75EBD0372BB91F3ECD C7089CE, as follow:

Download the PAM Self hosted document described above > go to Cyberark Portal cyberark.my.site.com/mplace/s/#software > choose Privileged Access Manager Self-Hosted > go to Components > choose Documentation > download Production-PublicHelp-PAS - 14.0.zip and Extract > choose OnlineHelp.htm > choose Install and Harden components

a) Install: Installation > install PAM Self-Hosted
b) Upgrade: Installation > Upgrade
c) Admin: Administrator > Components

1.3.1.2 Configuration List

The evaluation package consists of the following:

a) Privileged Access Manager – Digital Vault Server (TOE)
b) Privileged Access Manager – Digital Vault Server Security Target, v1.8
d) Privileged Access Manager – Digital Vault Server Entropy Description, v0.4
e) PAM Self-Hosted v14.0, 25-Jan-2024, No. A8474D5E4B6532ED3402D38B46F7DB15F650CA75EBD0372BB91F3ECD C7089CE.

1.3.1.3 Out-of-Scope Functionalities

The out-of-scope functionalities, which are disabled by default in the evaluated configuration are as follows:

a) Disaster Recovery Vault
b) Distributed Vault
c) Cluster Vault
d) PAM on Cloud
e) Backup (Replicate)
f) ENE (SMTP Monitoring)
g) HSM
h) Remote Control Client (SNMP Monitoring)
i) PAKeyGen
1.3.2 Logical Scope

The logical scope of the TOE comprises the security functions defined in section Security Functions.

1.4 Terminology

Table 2: Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CC</td>
<td>Common Criteria</td>
</tr>
<tr>
<td>CPM</td>
<td>CyberArk Central Policy Manager</td>
</tr>
<tr>
<td>CRL</td>
<td>Certificate Revocation List</td>
</tr>
<tr>
<td>CDP</td>
<td>CRL distribution point</td>
</tr>
<tr>
<td>DRBG</td>
<td>Deterministic Random Bit Generator</td>
</tr>
<tr>
<td>EAL</td>
<td>Evaluation Assurance Level</td>
</tr>
<tr>
<td>IIS</td>
<td>Internet information Services</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>NIAP</td>
<td>National Information Assurance Partnership</td>
</tr>
<tr>
<td>PP</td>
<td>Protection Profile</td>
</tr>
<tr>
<td>PAM</td>
<td>CyberArk Privileged Access Manager</td>
</tr>
<tr>
<td>PSM</td>
<td>CyberArk Privileged Session Manager</td>
</tr>
<tr>
<td>PSMP</td>
<td>CyberArk Privileged Session Manager SSH (Secure Shell) Proxy</td>
</tr>
<tr>
<td>PVWA</td>
<td>CyberArk Password Vault Web Access</td>
</tr>
<tr>
<td>SRP</td>
<td>Secure Remote Password</td>
</tr>
<tr>
<td>ST</td>
<td>Security Target</td>
</tr>
<tr>
<td>TOE</td>
<td>Target of Evaluation</td>
</tr>
<tr>
<td>TSF</td>
<td>TOE Security Functionality</td>
</tr>
</tbody>
</table>
## Conformance Claims

The following conformance claims are made:

1) CC version 3.1 Revision 5, April 2017
2) CC Part 2 extended, CCMB-2017-04-002, April 2017
3) CC Part 3 extended, CCMB-2017-04-003, April 2017
4) NIAP Protection Profile for Application Software, v1.4 (PP_APP), 2021-10-07
6) NIAP Technical Decisions per Table 3.

### Table 3: NIAP Technical Decisions

<table>
<thead>
<tr>
<th>TD Type</th>
<th>TD #</th>
<th>Name</th>
<th>Rationale if N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>PP_APP</td>
<td>TD0628</td>
<td>Addition of Container Image to Package Format</td>
<td></td>
</tr>
<tr>
<td>PP_APP</td>
<td>TD0650</td>
<td>Conformance claim sections updated to allow for MOD_VPNC_V2.3 and 2.4</td>
<td></td>
</tr>
<tr>
<td>PP_APP</td>
<td>TD0664</td>
<td>Testing activity for FPT_TUD_EXT.2.2</td>
<td></td>
</tr>
<tr>
<td>PP_APP</td>
<td>TD0717</td>
<td>Format changes for PP_APP_V1.4</td>
<td></td>
</tr>
<tr>
<td>PP_APP</td>
<td>TD0719</td>
<td>ECD for PP APP V1.3 and 1.4</td>
<td></td>
</tr>
<tr>
<td>PP_APP</td>
<td>TD0736</td>
<td>Number of elements for iterations of FCS_HTTPS_EXT.1</td>
<td>N/A. The TOE does not claim FCS_HTTPS_EXT.1/Server</td>
</tr>
<tr>
<td>PP_APP</td>
<td>TD0743</td>
<td>FTP_DIT_EXT.1.1 Selection exclusivity</td>
<td></td>
</tr>
<tr>
<td>PP_APP</td>
<td>TD0747</td>
<td>Configuration Storage Option for Android</td>
<td>N/A. the TOE is not an Android app</td>
</tr>
<tr>
<td>PP_APP</td>
<td>TD0756</td>
<td>Update for platform-provided full disk encryption</td>
<td></td>
</tr>
<tr>
<td>PP_APP</td>
<td>TD0780</td>
<td>FIA_X509_EXT.1 Test 4 Clarification</td>
<td>N/A. The TOE does not claim FIA_X509_EXT.1</td>
</tr>
<tr>
<td>PP_APP</td>
<td>TD0798</td>
<td>Static Memory Mapping Exceptions</td>
<td></td>
</tr>
<tr>
<td>PP_APP</td>
<td>TD0815</td>
<td>Addition of Conditional TSS Activity for FPT_AEX_EXT.1.5</td>
<td></td>
</tr>
<tr>
<td>PP_APP</td>
<td>TD0822</td>
<td>Correction to Windows Manifest File for FDP_DEC_EXT.1</td>
<td></td>
</tr>
<tr>
<td>TD Type</td>
<td>TD #</td>
<td>Name</td>
<td>Rationale if N/A</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>----------------------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>PP_APP</td>
<td>TD0823</td>
<td>Update to Microsoft Windows Exploit Protection link in FPT_AEX_EXT.1.3</td>
<td></td>
</tr>
<tr>
<td>PKG_TLS S_1.1</td>
<td>DT0779</td>
<td>Updated Session Resumption Support in TLS package V1.1</td>
<td></td>
</tr>
<tr>
<td>PKG_TLS S_1.1</td>
<td>TD0770</td>
<td>TLSS.2 connection with no client cert</td>
<td>NA, this SFR is not claimed</td>
</tr>
<tr>
<td>PKG_TLS S_1.1</td>
<td>TD0739</td>
<td>PKG_TLS_V1.1 has 2 different publication dates</td>
<td></td>
</tr>
<tr>
<td>PKG_TLS S_1.1</td>
<td>TD0726</td>
<td>Corrections to (D)TLSS SFRs in TLS 1.1 FP</td>
<td></td>
</tr>
<tr>
<td>PKG_TLS S_1.1</td>
<td>TD0513</td>
<td>CA Certificate loading</td>
<td></td>
</tr>
<tr>
<td>PKG_TLS S_1.1</td>
<td>TD0499</td>
<td>Testing with pinned certificates</td>
<td></td>
</tr>
<tr>
<td>PKG_TLS S_1.1</td>
<td>TD0469</td>
<td>Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1</td>
<td></td>
</tr>
<tr>
<td>PKG_TLS S_1.1</td>
<td>TD0442</td>
<td>Updated TLS Ciphersuites for TLS Package</td>
<td></td>
</tr>
</tbody>
</table>
3 Security Problem Definition

The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any organizational security policies that the TOE is expected to enforce.

3.1 Threats

Table 4: Threats

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>T.NETWORK_ATTACK</td>
<td>An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.</td>
</tr>
<tr>
<td>T.NETWORK_EAVESDROP</td>
<td>An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.</td>
</tr>
<tr>
<td>T.LOCAL_ATTACK</td>
<td>An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.</td>
</tr>
<tr>
<td>T PHYSICAL_ACCESS</td>
<td>An attacker may try to access sensitive data at rest.</td>
</tr>
</tbody>
</table>

3.2 Assumptions

Table 5: Assumptions

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.PLATFORM</td>
<td>The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.</td>
</tr>
<tr>
<td>A.PROPER_USER</td>
<td>The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.</td>
</tr>
<tr>
<td>A.PROPER_ADMIN</td>
<td>The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.</td>
</tr>
</tbody>
</table>

3.3 Organizational Security Policies

There are no organizational security policies for the application.
## 4 Security Objectives

### 4.1 Objectives for the TOE

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>O.INTEGRITY</td>
<td>Conformant TOEs ensure the integrity of their installation and update packages, and also leverage execution environment-based mitigations. Software is seldom, if ever, shipped without errors. The ability to deploy patches and updates to fielded software with integrity is critical to enterprise network security. Processor manufacturers, compiler developers, execution environment vendors, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Application software can often take advantage of these mechanisms by using APIs provided by the runtime environment or by enabling the mechanism through compiler or linker options.</td>
</tr>
<tr>
<td>O.QUALITY</td>
<td>To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex operations such as file and media parsing. Leveraging this platform behaviour relies upon using only documented and supported APIs.</td>
</tr>
<tr>
<td>O.MANAGEMENT</td>
<td>To facilitate management by users and the enterprise, conformant TOEs provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration. This also includes providing control to the user regarding disclosure of any PII.</td>
</tr>
<tr>
<td>O.PROTECTED_STORAGE</td>
<td>To address the issue of loss of confidentiality of user data in the event of loss of physical control of the storage medium, conformant TOEs will use data-at-rest protection. This involves encrypting data and keys stored by the TOE in order to prevent unauthorized access to this data. This also includes unnecessary network communications whose consequence may be the loss of data.</td>
</tr>
<tr>
<td>O.PROTECTED_COMMS</td>
<td>To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOEs use a trusted channel for sensitive data. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application.</td>
</tr>
</tbody>
</table>
## 4.2 Objectives for the Operational Environment

### Table 7: Operational environment objectives

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OE.PLATFORM</td>
<td>The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.</td>
</tr>
<tr>
<td>OE.PROPER_USER</td>
<td>The user of the application software is not wilfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.</td>
</tr>
<tr>
<td>OE.PROPER_ADMIN</td>
<td>The administrator of the application software is not careless, wilfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.</td>
</tr>
</tbody>
</table>
5 Security Requirements

5.1 Conventions

This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with italicized text in square brackets.

b) **Refinement.** Indicated with bold text and strikethroughs in square brackets.

c) **Selection.** Indicated with underlined text in square brackets.

d) **Assignment within a selection.** Indicated with italicized and underlined text in square brackets.

e) **Iteration.** Indicated by adding a slash and a name, e.g., “FCS_COP.1/Hash”.

5.2 Extended Components Definition

All extended components (identified by EXT) are reproduced directly from the claimed Protection Profile and therefore no further definition is provided in this document.

5.3 Functional Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Title</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCS_CKM.1/AK</td>
<td>Cryptographic Asymmetric Key Generation</td>
<td>Selection</td>
</tr>
<tr>
<td>FCS_CKM_EXT.1</td>
<td>Cryptographic Key Generation Services</td>
<td>Mandatory</td>
</tr>
<tr>
<td>FCS_CKM.2</td>
<td>Cryptographic Key Establishment</td>
<td>Selection</td>
</tr>
<tr>
<td>FCS_COP.1/SKC</td>
<td>Cryptographic Operation – Encryption/Decryption</td>
<td>Selection</td>
</tr>
<tr>
<td>FCS_COP.1/Hash</td>
<td>Cryptographic Operation – Hashing</td>
<td>Selection</td>
</tr>
<tr>
<td>FCS_COP.1/Sig</td>
<td>Cryptographic Operation – Signing</td>
<td>Selection</td>
</tr>
<tr>
<td>FCS_COP.1/KeyedHash</td>
<td>Cryptographic Operation – Keyed-Hash Message Authentication</td>
<td>Selection</td>
</tr>
<tr>
<td>FCS_RBG_EXT.1</td>
<td>Random Bit Generation Services</td>
<td>Mandatory</td>
</tr>
<tr>
<td>FCS_STO_EXT.1</td>
<td>Storage of Credentials</td>
<td>Mandatory</td>
</tr>
<tr>
<td>FCS_TLS_EXT.1</td>
<td>TLS Protocol</td>
<td>Mandatory</td>
</tr>
<tr>
<td>FCS_TLSS_EXT.1</td>
<td>TLS Server Protocol</td>
<td>Selection</td>
</tr>
<tr>
<td>FDP_DEC_EXT.1</td>
<td>Access to Platform Resources</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Requirement</td>
<td>Title</td>
<td>Type</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>FDP_NET_EXT.1</td>
<td>Network Communications</td>
<td>Mandatory</td>
</tr>
<tr>
<td>FDP_DAR_EXT.1</td>
<td>Encryption Of Sensitive Application Data</td>
<td>Mandatory</td>
</tr>
<tr>
<td>FMT_MEC_EXT.1</td>
<td>Supported Configuration Mechanism</td>
<td>Mandatory</td>
</tr>
<tr>
<td>FMT_CFG_EXT.1</td>
<td>Secure by Default Configuration</td>
<td>Mandatory</td>
</tr>
<tr>
<td>FMT_SMF.1</td>
<td>Specification of Management Functions</td>
<td>Mandatory</td>
</tr>
<tr>
<td>FPR_ANO_EXT.1</td>
<td>User Consent for Transmission of Personally Identifiable Information</td>
<td>Mandatory</td>
</tr>
<tr>
<td>FPT_API_EXT.1</td>
<td>Use of Supported Services and APIs</td>
<td>Mandatory</td>
</tr>
<tr>
<td>FPT_AEX_EXT.1</td>
<td>Anti-Exploitation Capabilities</td>
<td>Mandatory</td>
</tr>
<tr>
<td>FPT_TUD_EXT.1</td>
<td>Integrity for Installation and Update</td>
<td>Mandatory</td>
</tr>
<tr>
<td>FPT_TUD_EXT.2</td>
<td>Integrity for Installation and Update</td>
<td>Selection</td>
</tr>
<tr>
<td>FPT_LIB_EXT.1</td>
<td>Use of Third-Party Libraries</td>
<td>Mandatory</td>
</tr>
<tr>
<td>FPT_IDV_EXT.1</td>
<td>Software Identification and Versions</td>
<td>Mandatory</td>
</tr>
<tr>
<td>FTP_DIT_EXT.1</td>
<td>Protection of Data in Transit</td>
<td>Mandatory</td>
</tr>
</tbody>
</table>

### 5.3.1 Cryptographic Support (FCS)

**FCS_CKM.1/AK**  **Cryptographic Asymmetric Key Generation**

FCS_CKM.1.1/AK  The application shall [implement functionality] to generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm [

- **[ECC schemes]** using [“NIST curves” P-384 and P-256] that meet the following: [FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4].

].

Application Note: This SFR was altered by TD0717.

**FCS_CKM_EXT.1**  **Cryptographic Key Generation Services**

FCS_CKM_EXT.1.1  The application shall [implement asymmetric key generation].

Application Note: This SFR was altered by TD0717.
FCS_CKM.2  Cryptographic Key Establishment

FCS_CKM.2.1 The application shall \[implement functionality\] to perform cryptographic key establishment in accordance with a specified cryptographic key establishment method:\[
\begin{itemize}
  \item \[Elliptic curve-based key establishment schemes\] that meets the following: \[NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”\].
  \item \[FFC Schemes using “safe-prime” groups\] that meet the following: \[NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [RFC 7919]\].
\end{itemize}\]

FCS_COP.1/SKC  Cryptographic Operation – Encryption/Decryption

FCS_COP.1.1/SKC The application shall perform \[encryption/decryption\] in accordance with a specified cryptographic algorithm:\[
\begin{itemize}
  \item AES-CBC (as defined in NIST SP 800-38A) mode,
  \item AES-GCM (as defined in NIST SP 800-38D) mode.
\end{itemize}\] and cryptographic key sizes \[128-bit, 256-bit\].

Application note: This SFR was altered by TD0717.

FCS_COP.1/Hash  Cryptographic Operation – Hashing

FCS_COP.1.1/Hash The application shall perform \[cryptographic hashing services\] in accordance with a specified cryptographic algorithm:\[
\begin{itemize}
  \item SHA-256,
  \item SHA-384,
  \item SHA-512
\end{itemize}\] and \textbf{message digest} sizes:\[
\begin{itemize}
  \item 256,
  \item 384,
  \item 512
\end{itemize}\] bits that meet the following: \[FIPS Pub 180-4\].

FCS_COP.1/Sig  Cryptographic Operation – Signing

FCS_COP.1.1/Sig The \textbf{application} shall perform \[cryptographic signature services \textit{(generation and verification)}\] in accordance with a specified cryptographic algorithm:\[
\begin{itemize}
  \item \[..\]
\end{itemize}\]
- **RSA schemes** using cryptographic key sizes of [2048-bit or greater] that meet the following: [FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5].

Application note: This SFR was altered by TD0717.

**FCS_COP.1/KeyedHash**  
**Cryptographic Operation – Keyed-Hash Message Authentication**

**FCS_COP.1.1/KeyedHash**  
The application shall perform [keyed-hash message authentication] in accordance with a specified cryptographic algorithm [  
- HMAC-SHA-256  
- HMAC-SHA-384  
- HMAC-SHA-512  
] and [  
- no other algorithms  
] with key sizes [256, 384, 512] and message digest sizes [256, 384, 512] and [no other size] bits that meet the following: [FIPS Pub 198-1, 'The Keyed-Hash Message Authentication Code' and FIPS Pub 180-4 'Secure Hash Standard'].

Application note: This SFR was altered by TD0717.

**FCS_RBG_EXT.1**  
**Random Bit Generation Services**

**FCS_RBG_EXT.1.1**  
The application shall [invoke platform-provided DRBG functionality] for its cryptographic operations.

**FCS_STO_EXT.1**  
**Storage of Credentials**

**FCS_STO_EXT.1.1**  
The application shall [implement functionality to securely store [file keys, safe keys, and password verifiers] according to [FCS_COP.1/SKC]] to non-volatile memory.

**FCS_TLS_EXT.1**  
**TLS Protocol**

**FCS_TLS_EXT.1.1**  
The product shall implement [  
- TLS as a server  
].

**FCS_TLSS_EXT.1**  
**TLS Server Protocol**

**FCS_TLSS_EXT.1.1**  
The product shall implement TLS 1.2 (RFC 5246) and [no earlier TLS versions] as a server that supports the cipher suites [  

Page 17 of 68
• TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
• TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
• TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288

] and no other cipher suites, and also supports functionality for [ 
• none
].

Application Note: This SFR was altered by TD0779

FCS_TLSS_EXT.1.2 The product shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [TLS 1.1]

FCS_TLSS_EXT.1.3 The product shall perform key establishment for TLS using [ 
• Diffie-Hellman parameters with size [3072 bits] and no other sizes,
• ECDHE parameters using elliptic curves [secp256r1, secp384r1] and no other curves.
].

Application Note: This SFR was altered by TD0726.

5.3.2 User Data Protection (FDP)

FDP_DEC_EXT.1 Access to Platform Resources
FDP_DEC_EXT.1.1 The application shall restrict its access to [ 
• network connectivity
].

FDP_DEC_EXT.1.2 The application shall restrict its access to [ 
• [the firewall, and event and system log repositories]
].

FDP_NET_EXT.1 Network Communications
FDP_NET_EXT.1.1 The application shall restrict network communication to [ 
• user-initiated communication for [the establishment of TLS sessions with the PAM components and the following functions:
  o CPM – authenticate to Password Vault Server, retrieve and update privileged passwords and password policies
].

Page 18 of 68
CyberArk Security Target

PSM – authenticate to Password Vault Server, retrieve privileged accounts, upload privileged session recordings

PVWA – authenticate to Password Vault Server, TOE administration

PSMP – authenticate to Password Vault Server, retrieve privileged accounts, upload privileged session recordings.

FDP_DAR_EXT.1 Encryption Of Sensitive Application Data

The application shall [leverage platform-provided functionality to encrypt sensitive data, protect sensitive data in accordance with FCS_STO_EXT.1] in non-volatile memory.

5.3.3 Security Management (FMT)

FMT_MEC_EXT.1 Supported Configuration Mechanism

The application shall [invoke the mechanisms recommended by the platform vendor for storing and setting configuration options].

FMT_CFG_EXT.1 Secure by Default Configuration

The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.

The application shall be configured by default with file permissions which protect the application binaries and data files from modification by normal unprivileged users.

FMT_SMF.1 Specification of Management Functions

The TSF shall be capable of performing the following management functions [user management, configuration management, password management, start/stop service].

5.3.4 Privacy (FPR)

FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information

The application shall [not transmit PII over a network].
5.3.5 Protection of the TSF (FPT)

FPT_API_EXT.1 Use of Supported Services and APIs

FPT_API_EXT.1.1 The application shall use only documented platform APIs.

FPT_AEX_EXT.1 Anti-Exploitation Capabilities

FPT_AEX_EXT.1.1 The application shall not request to map memory at an explicit address except for:
- 0x0000000000000000
- 0x000000007FFF0000
- 0x000000007FFE0000
- 0x000000007FFE1000
- 0x000000007FFE3000

FPT_AEX_EXT.1.2 The application shall not allocate any memory region with both write and execute permissions.

FPT_AEX_EXT.1.3 The application shall be compatible with security features provided by the platform vendor.

FPT_AEX_EXT.1.4 The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.

FPT_AEX_EXT.1.5 The application shall be built with stack-based buffer overflow protection enabled.

FPT_TUD_EXT.1 Integrity for Installation and Update

FPT_TUD_EXT.1.1 The application shall leverage the platform to check for updates and patches to the application software.

FPT_TUD_EXT.1.2 The application shall provide the ability to view the current version of the application software.

FPT_TUD_EXT.1.3 The application shall not download, modify, replace or update its own binary code.

FPT_TUD_EXT.1.4 Application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.

FPT_TUD_EXT.1.5 The application is distributed as an additional software package to the platform OS.
FPT_TUD_EXT.2.1 The application shall be distributed using the format of the platform-supported package manager.

FPT_TUD_EXT.2.2 The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.

FPT_TUD_EXT.2.3 The application installation package shall be digitally signed such that its platform can cryptographically verify them prior to installation.

FPT_LIB_EXT.1 Use of Third Party Libraries

FPT_LIB_EXT.1.1 The application shall be packaged with only [the libraries listed in Appendix B].

FPT_IDV_EXT.1 Software Identification and Versions

FPT_IDV_EXT.1.1 The application shall be versioned with [[version number]].

5.3.6 Trusted Path/Channel (FTP)

FTP_DIT_EXT.1 Protection of Data in Transit

FTP_DIT_EXT.1.1 The application shall [encrypt all transmitted [sensitive data] with [TLS as a server as defined in the Functional Package for TLS and also supports functionality for [none],] between itself and another trusted IT product. ]
5.4 Assurance Requirements

The TOE security assurance requirements are summarized in Table 9.

<table>
<thead>
<tr>
<th>Assurance Class</th>
<th>Components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Target Evaluation</td>
<td>ASE_CCL.1</td>
<td>Conformance Claims</td>
</tr>
<tr>
<td></td>
<td>ASE_ECD.1</td>
<td>Extended Components Definition</td>
</tr>
<tr>
<td></td>
<td>ASE_INT.1</td>
<td>ST Introduction</td>
</tr>
<tr>
<td></td>
<td>ASE_OBJ.1</td>
<td>Security Objectives for the operational environment</td>
</tr>
<tr>
<td></td>
<td>ASE_REQ.1</td>
<td>Stated Security Requirements</td>
</tr>
<tr>
<td></td>
<td>ASE_SPD.1</td>
<td>Security Problem Definition</td>
</tr>
<tr>
<td></td>
<td>ASE_TSS.1</td>
<td>TOE Summary Specification</td>
</tr>
<tr>
<td>Development</td>
<td>ADV_FSP.1</td>
<td>Basic Functional Specification</td>
</tr>
<tr>
<td>Guidance Documents</td>
<td>AGD_OPE.1</td>
<td>Operational User Guidance</td>
</tr>
<tr>
<td></td>
<td>AGD_PRE.1</td>
<td>Preparative User Guidance</td>
</tr>
<tr>
<td>Life Cycle Support</td>
<td>ALC_CMC.1</td>
<td>Labelling of the TOE</td>
</tr>
<tr>
<td></td>
<td>ALC_CM.1</td>
<td>TOE CM Coverage</td>
</tr>
<tr>
<td></td>
<td>ALC_TSU_EXT.1</td>
<td>Timely Security Updates (as defined in PP_APP)</td>
</tr>
<tr>
<td>Tests</td>
<td>ATE_IND.1</td>
<td>Independent Testing – conformance</td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td>AVA_VAN.1</td>
<td>Vulnerability Analysis</td>
</tr>
</tbody>
</table>
6 TOE Summary Specification

6.1 Timely Security Updates

CyberArk endeavors to remediate critical and high severity publicly disclosed vulnerabilities in its TOEs, in accordance with their severity as implemented in the TOE, and subject to patches made available by their respective vendors (if applicable). The security updated can be provided as quickly as 4 weeks.

CyberArk will report a vulnerability to its customers when customers are required to take action to apply the remediation. Reporting of vulnerability-related issues may be via a security bulletin, release notes, knowledge base article, in-product notification or any other appropriate notification method. For the protection of CyberArk’s customers, reporting of a vulnerability (including disclosure to any individual customer) will only be made once a remediation is made generally available by CyberArk, unless otherwise required by applicable law or regulation. In addition, the level of detail regarding a vulnerability in any reporting will be limited only to the minimum necessary.

If a security bulletin is issued, notification is sent via email to our technical subscribers (defined per customer upon request) and also published on the CyberArk website - Product Security | CyberArk, leading to a password-protected technical community - Login (site.com). First time users are asked to register prior to login.

6.2 SFR Fulfilment

Table 10 describes how the TOE fulfils the SFRs.

<table>
<thead>
<tr>
<th>SFR</th>
<th>Fulfilment</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCS_CKM.1/AK</td>
<td>Table 11 below lists all the key sizes used for the ECC asymmetric key generation scheme and its usage. Table 11 also lists the key establishment and key exchange schemes used by the TOE.</td>
</tr>
<tr>
<td>FCS_CKM_EXT.1</td>
<td>The TOE uses ECDHE and DHE key establishment/exchange for TLS. The use of asymmetric encryption is needed for the TLS protocol used by the TOE. The key generation methods follow the requirements within FIPS PUB 186-4. The key establishment methods follow the requirements within NIST Special Publication 800-56A.</td>
</tr>
<tr>
<td>FCS_CKM.2</td>
<td>AES128-CBC, AES256-CBC, AES128-GCM, AES256-GCM is used for the encryption/decryption of sensitive data stored in non-volatile memory.</td>
</tr>
<tr>
<td>FCS_COP.1/SKC</td>
<td>Table 12 lists all the key sizes used for SHA hashing and message digests within the TOE. SHA is used in TLS and SRP. The SHA256, SHA384, and SHA512 hash functions are used in HMAC for TLS message integrity and authentication. The TOE’s implementation of SHA follows the requirements within FIPS Pub 180-4.</td>
</tr>
<tr>
<td>SFR</td>
<td>Fulfilment</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>FCS_COP.1/Sig</td>
<td>Table 11 lists all the key sizes used for signature generation and verification for TLS and the key sizes used to verify TOE file signatures. The TOE’s implementation of signature generation and verification follow the requirements within FIPS PUB 186-4.</td>
</tr>
<tr>
<td>FCS_COP.1/KeyedHash</td>
<td>Table 12 lists all the key sizes used for SHA hashing and message digests within the TOE. SHA is used in TLS and SRP. The SHA256, SHA384, and SHA512 hash functions are used in HMAC for TLS message integrity and authentication. The TOE’s implementation of SHA follows the requirements within FIPS Pub 180-4.</td>
</tr>
<tr>
<td>FCS_RBG_EXT.1</td>
<td>The TOE implements the Approved SP 800-90 Approved AES256-CTR DRBG to generate random bits for key generation. When the TOE starts up, the DRBG is seeded with 256 bits of entropy from the Windows Entropy Pool by calling the OpenSSL RAND_seed function for the CryptGenRandom function and for Crypto API (CAPI). The platform system time and tick count noise sources are added to the Windows OS Entropy Pool after initialization. On an ongoing basis the TOE seeds the DRBG with 256 bits of entropy by calling the RAND_seed function for the BCryptGenRandom function and for the CNG (Crypto Next Generation) API. More information about the entropy process is described in the proprietary Entropy Rationale document.</td>
</tr>
</tbody>
</table>
| FCS_STO_EXT.1       | The TOE secures sensitive data stored in non-volatile memory using its algorithms for AES256-CBC encryption with a 256-bit key. Sensitive data includes the file key sent with a file from a PAM component, the Safe key used to encrypt the file key, and the verifier associated with a CyberArk password (for CyberArk authentication).  
  - The privileged account file sent by a PAM client is encrypted by the PAM client.  
  - The encrypted file is sent to the TOE and the file key is sent along securely in encrypted form over TLS.  
  - The TOE decrypts the file key, then encrypts the file key with the Safe’s unique AES 256-bit key using AES256-CBC encryption.  
  - The Safe key is encrypted by the unique AES 256-bit Server key and stored within the Safe. A Safe key is generated automatically using the DRBG when a Safe is created.  
  
An administrator creates the initial password for a CyberArk (local) account. When the administrator creates the initial password, or a user changes it, the password is concatenated and manipulated using hash and exponential functions to derive a password verifier.  
The password verifier is stored in the MySQL DB. In the MySQL DB, the column containing the verifier is encrypted with the Server key using AES256-CBC encryption.  
Any time a local user authenticates, the password verifier is derived and authenticated against the value stored in the DB. |
<table>
<thead>
<tr>
<th>SFR</th>
<th>Fulfilment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The Server key is unique to the TOE and is stored in volatile memory. The Server key is used to encrypt the Safe keys and the sensitive data stored within the DB. A Safe key is used to encrypt one or more files within a Safe.</td>
</tr>
<tr>
<td></td>
<td>The Administrator user, and the PAM component users listed below, authenticate to the TOE using CyberArk authentication:</td>
</tr>
<tr>
<td></td>
<td>• CPM – PasswordManager</td>
</tr>
<tr>
<td></td>
<td>• PVWA – PVWAppUser, PVWAGWUser</td>
</tr>
<tr>
<td></td>
<td>• PSM – PSMAPPUser, PSMGWUser</td>
</tr>
<tr>
<td></td>
<td>• PSMP – PSMPAppUser, PSMPGWUser</td>
</tr>
<tr>
<td>FCS_TLS_EXT.1</td>
<td>The TOE is a server to the OE PAM component clients. The TOE uses the <a href="https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/details?product=14798">https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/details?product=14798</a> CyberArk Cryptographic Module v2.2.1 Module with the CyberArk libraries for the cryptographic services required to support TLS communications with the PAM component clients.</td>
</tr>
<tr>
<td>FCS_TLSS_EXT.1</td>
<td>The TOE uses X.509v3 certificates for TLS communications. The certificates are presented by the TOE during the TLS handshake is established. The vault certificates are authenticated by the connecting client, i.e. the Windows server PAM components, and the Linux server PAM components. The certificates can include (per generation) a CRL distribution point (CDP) to enable the clients to use a certificate revocation list (CRL) mechanisms to verify the certificate.</td>
</tr>
<tr>
<td></td>
<td>The TOE supports:</td>
</tr>
<tr>
<td></td>
<td>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</td>
</tr>
<tr>
<td></td>
<td>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td></td>
<td>Six TLS suites are suggested by the components during the TLS handshake. These are:</td>
</tr>
<tr>
<td></td>
<td>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384</td>
</tr>
<tr>
<td></td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128-GCM-SHA256</td>
</tr>
<tr>
<td></td>
<td>From these, the Vault server does not support ECDSA certificates. From the remaining four suites, the vault server will always select the strongest one available - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384.</td>
</tr>
</tbody>
</table>
Therefore, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 is the only ciphersuite used.

The TOE does not accept any connection requests using SSL or a TLS version other than TLSv1.2. The TOE checks that the presented identifier matches the reference identifier, either the IP or DNS name, and only establishes a trusted channel if the identifier is a match and if the client’s certificate is validated. The TOE supports certificate pinning. Key agreement parameters are provided in Table 11: Cryptographic Algorithms.

### SFR Fulfilment

<table>
<thead>
<tr>
<th>FDP_DEC_EXT.1</th>
<th>The TOE limits its access to only network connectivity when accessing the platform’s hardware resources. The TOE requires network access to the CA server, the Windows server PAM components, and the RHEL server PAM components.</th>
</tr>
</thead>
<tbody>
<tr>
<td>FDP_NET_EXT.1</td>
<td>The TOE limits access to only network connectivity between the PAM component clients and the TOE over TLS on port 443. The TOE also uses port 80 for HTTP connections to the CA server for certification revocation checks. The TOE limits access to the platform's firewall services and audit mechanism. The TOE hardening process closes all ports and removes services not required by the TOE. The TOE accesses the platform’s firewall to take control over the firewall services and change the firewall information flow control rules. The TOE also accesses the platform’s audit mechanism to write event and system logs.</td>
</tr>
<tr>
<td>FDP_DAR_EXT.1</td>
<td>With the exception of cryptographic key destruction for keys stored in volatile memory, the TOE does not depend on platform-provided cryptographic functionality to provide its cryptographic services. The cryptographic functionality is included with the CyberArk Crypto Library, which provides all cryptographic services including encryption/decryption of data stored in Safes and in the MySQL DB. The TOE protects sensitive data by using AES256-CBC to encrypt the data before storing it in non-volatile memory and restricting access to the data. Sensitive data includes the file key used to encrypt a file sent by a PAM client, the Safe key used to encrypt the file key, and the password verifier used for SRP authentication to the TOE. The file key is encrypted by the Safe key of the Safe where it is stored. Both the client file and its encrypted file key are stored within the Safe. All sensitive data stored within a Safe is protected by that Safe’s key. The Safes are stored in non-volatile memory at c:\Private\Safes. The Safe key is encrypted with the 256-bit Server key using AES256-CBC encryption. The Server key is stored in volatile memory. The Administrator user and PAM components use SRP authentication. PAM client password verifiers are encrypted with the Server key using AES256-CBC encryption and stored in the MySQL DB. The sensitive data within a Safe is protected by the combination of the Vault Access Control Policy,</td>
</tr>
<tr>
<td>SFR</td>
<td>Fulfilment</td>
</tr>
<tr>
<td>-----</td>
<td>------------</td>
</tr>
<tr>
<td></td>
<td>which is configured by the installation process, and the Safe Access Control Policy. Access to the Vault and Safes is enforced by user account authorizations and permissions. The Vault Access Control Policy controls user access to the Vault. The Vault Access Control Policy only allows access to the Vault for those users that are defined in the Vault.ini file. The Safe Access Control Policy controls Safe member permissions to view or create Safes and their permissions on the files within the Safes. An operator attempting to access the Vault or Safes with the incorrect authorizations and permissions is denied access. PSM and PSMP recordings may contain sensitive information if the user chooses to connect to a remote target which may contain sensitive information, therefore, we recommend the user to enable BitLocker.</td>
</tr>
<tr>
<td>FMT_MEC_EXT.1</td>
<td>The TOE uses OS functionality for storing and setting configuration options. The storage location of configuration files is maintained in the Windows Registry. The Server Windows Registry entries are located in the following file: HKLM\Software\CyberArk\PrivateArk\Server. The TOE contains local configuration files that are created during installation, but the information is read-only and never written to by the TOE. The Administrator user or users in the Administrators group have Full control, Modify, Read &amp; Execute, Read, and Write permissions for the configuration files. The configuration files are located in the C:\Program Files (x86)\PrivateArk\Server\conf folder. The DBParm.ini configuration file contains the general parameters for the Vault database. This file contains parameters for cryptographic algorithms, key locations, certificate settings, groups and users, and the TOE's listening port. The Passparm.ini file contains the password complexity settings.</td>
</tr>
<tr>
<td>FMT_CFG_EXT.1</td>
<td>Physical access is required for installation of the TOE. The TOE provides only enough functionality to enter credentials for the Administrator and Master users during installation. There are no default credentials for these users and no other default credentials stored on the TOE. Only an authorized administrator can install the TOE and set the credentials. During installation, the TOE is configured by default to protect the application’s files from unauthorized access. The files are set with permissions that do not allow the Users group to modify them.</td>
</tr>
<tr>
<td>FMT_SMF.1</td>
<td>The TOE provides the following management functions: user management, configuration management, password management, start/stop service. Any other management operations must be performed by an authorized administrator using PVWA in the environment.</td>
</tr>
<tr>
<td>FPR_ANO_EXT.1</td>
<td>The TOE does not transmit PII. Usernames were considered and determined to not be PII as this information is owned and generated by the company that implements the TOE. This means that a Security</td>
</tr>
<tr>
<td>SFR</td>
<td>Fulfilment</td>
</tr>
<tr>
<td>-----</td>
<td>------------</td>
</tr>
<tr>
<td></td>
<td>Policy must be enforced by the company that implements the TOE to prevent users from choosing their own personal username that could link to their personal identity.</td>
</tr>
<tr>
<td>FPT_API_EXT.1</td>
<td>The TOE uses only the standard platform APIs. Refer to Appendix A for a list of all APIs used by the TOE.</td>
</tr>
</tbody>
</table>
| FPT_AEX_EXT.1 | The TOE provides anti-exploitation protections. By default, ASLR protection is enabled on the Windows 2019 server. The TOE is compiled using the /NXCOMPAT flag to enable Data Execution Protection (DEP) and the /GS flag to enable stack-based buffer overflow protection. The TOE does not write user-modifiable files to directories that contain executable files.  
  - Executable files are stored in `\PrivateArk\Server\`.  
  - User-modifiable files are written to `\PrivateArk\Server\Conf` and `\PrivateArk\Server\Logs`. |
| FPT_TUD_EXT.1/2 FPT_IDV_EXT.1 | The TOE is delivered through CyberArk’s online customer portal, which uses AWS Marketplace. The TOE installation and configuration files are all packaged into a zip file that is digitally signed by CyberArk. To verify the digital signature of a TOE package, users must do the following:  
  1. Download the TOE installation package from CyberArk.  
  2. Download and install the Java Development Kit (JDK) from Oracle.  
  3. Download and install the JCE Unlimited Strength Jurisdiction Policy Files.  
  4. Run the following command: `JDK_Home%/jarsigner.exe -verify -verbose -certs .zip`.  
     More information about the jarsigner's options can be found at [https://docs.oracle.com/javase/7/docs/technotes/tools/windows/jarsigner.html#CCHFIDAB](https://docs.oracle.com/javase/7/docs/technotes/tools/windows/jarsigner.html#CCHFIDAB).  
     Individual TOE files are signed using the Windows OS package manager MS21 Sign tool. To verify the integrity of the TOE installation file, do the following:  
     1. Extract the files from the archive file.  
     2. Navigate to the setup.exe file.  
     3. Right-click the file, then click **Properties > Digital Signatures**. |
4. Select the **CyberArk Software Ltd.** signer. Click **Details**, and then verify the signature details.

The authorized signing source is CyberArk.

The TOE relies on the platform's package manager to make changes to the binary code. Installation of the updates is performed by an administrator while using the executable file (.exe) extracted from the archive file (.zip).

You can remove the TOE software from the platform using the platform’s Programs and Features manager. Uninstallation of the TOE removes all traces of the application except for configuration settings, output files, and audit/log events.

You can obtain the TOE version number by navigating to `C:\CyberArk\Server_rls`.

Versioning naming convention: **AA.B.C.DD** (e.g: 14.0.0.32)

- **AA** – Major Version Number – 14
- **B** – Minor Version Number – 0
- **C** – Patch Number – 0
- **DD** – Build Number - 32

<table>
<thead>
<tr>
<th>FPT_LIB_EXT.1</th>
<th>The TOE is packaged with third-party libraries required for its functionality. For a full list, refer to Appendix B.</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP_DIT_EXT.1</td>
<td>The TOE protects data in transit by providing trusted paths and channels using the cryptographic functions within the TOE’s CyberArk PAM Cryptographic libraries. Communications between the TOE and Windows server’s CPM, PSM, PVWA PAM components and between the TOE and RHEL server’s PSMP PAM components are protected by TLS. The TOE acts as TLS server to the CPM, PSM, PVWA Windows components and to the PSMP PAM RHEL component. There is a single channel between the components and the TOE using TCP port 443.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 11: Cryptographic Algorithms</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>Encryption/Decryption</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Key Generation</td>
</tr>
<tr>
<td>Operation</td>
</tr>
<tr>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Signature Generation</td>
</tr>
<tr>
<td>Signature Verification</td>
</tr>
<tr>
<td>Key Exchange /Establishment</td>
</tr>
<tr>
<td>Message Digest</td>
</tr>
<tr>
<td>Message Authentication</td>
</tr>
<tr>
<td>Random Number Generation</td>
</tr>
</tbody>
</table>

Table 12: HMAC

<table>
<thead>
<tr>
<th>Hash Function</th>
<th>Block Size</th>
<th>Key Length</th>
<th>Output Digest</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA256</td>
<td>512</td>
<td>256</td>
<td>256</td>
</tr>
<tr>
<td>SHA384</td>
<td>1024</td>
<td>384</td>
<td>384</td>
</tr>
<tr>
<td>SHA512</td>
<td>1024</td>
<td>512</td>
<td>512</td>
</tr>
</tbody>
</table>
7 Rationale

7.1 Conformance Claim Rationale

The following rationale is presented with regard to the PP conformance claims:

a) **TOE type.** As identified in section 1.2.1, the TOE is an application, consistent with the PP.

b) **Security problem definition.** As shown in section 3, the threats, OSPs and assumptions are reproduced in this ST.

c) **Security objectives.** As shown in section 4, the security objectives are reproduced in this ST.

d) **Security requirements.** As shown in section 5, the security requirements are reproduced from the PP. No additional requirements have been specified.

7.2 Security Objectives Rationale

All security objectives are drawn directly from the claimed PP.

<table>
<thead>
<tr>
<th>Threat, Assumption, or OSP</th>
<th>Security Objectives</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>T.NETWORK_ATTACK</td>
<td>O.PROTECTED_COMMS, O.INTEGRITY, O.MANAGEMENT</td>
<td>The threat T.NETWORK_ATTACK is countered by O.PROTECTED_COMMS because this provides for integrity of transmitted data. The threat T.NETWORK_ATTACK is countered by O.INTEGRITY because this provides for integrity of software that is installed onto the system from the network. The threat T.NETWORK_ATTACK is countered by O.MANAGEMENT because this provides for the ability to configure the application to defend against network attack.</td>
</tr>
<tr>
<td>T.NETWORK_EAVESDROP</td>
<td>O.PROTECTED_COMMS, O.QUALITY, O.MANAGEMENT</td>
<td>The threat T.NETWORK_EAVESDROP is countered by O.PROTECTED_COMMS because this provides for confidentiality of transmitted data. The objective O.QUALITY ensures use of mechanisms that provide protection against network-based attack. The threat T.NETWORK_EAVESDROP is</td>
</tr>
<tr>
<td>Threat, Assumption, or OSP</td>
<td>Security Objectives</td>
<td>Rationale</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>O.MANAGEMENT</td>
<td>countered by O.MANAGEMENT because this provides for the ability to configure the application to protect the confidentiality of its transmitted data.</td>
</tr>
<tr>
<td>T.LOCAL_ATTACK</td>
<td>O.QUALITY</td>
<td>The objective O.QUALITY protects against the use of mechanisms that weaken the TOE with regard to attack by other software on the platform.</td>
</tr>
<tr>
<td>T.PHYSICAL_ACCESS</td>
<td>O.PROTECTED_STORAGE</td>
<td>The objective O.PROTECTED_STORAGE protects against unauthorized attempts to access physical storage used by the TOE.</td>
</tr>
<tr>
<td>A.PLATFORM</td>
<td>OE.PLATFORM</td>
<td>The operational environment objective OE.PLATFORM is realized through A.PLATFORM.</td>
</tr>
<tr>
<td>A.PROPER_USER</td>
<td>OE.PROPER_USER</td>
<td>The operational environment objective OE.PROPER_USER is realized through A.PROPER_USER.</td>
</tr>
<tr>
<td>A.PROPER_ADMIN</td>
<td>OE.PROPER_ADMIN</td>
<td>The operational environment objective OE.PROPER_ADMIN is realized through A.PROPER_ADMIN.</td>
</tr>
</tbody>
</table>

### 7.3 Security Requirements Rationale

All security requirements are drawn directly from the claimed PP.
8 Appendix A

Platform API for dbmain.exe version 14.0.0.40

Contents of this file

1) Platform modules used
2) Platform API used per module

*** 1) Platform modules used ***

ADVAPI32.DLL
API-MS-WIN-CRT-CONIO-L1-1-0.DLL
API-MS-WIN-CRT-CONVERT-L1-1-0.DLL
API-MS-WIN-CRT-ENVIRONMENT-L1-1-0.DLL
API-MS-WIN-CRT-FILESYSTEM-L1-1-0.DLL
API-MS-WIN-CRT-HEAP-L1-1-0.DLL
API-MS-WIN-CRT-LOCAL-E-L1-1-0.DLL
API-MS-WIN-CRT-MATH-L1-1-0.DLL
API-MS-WIN-CRT-RUNTIME-L1-1-0.DLL
API-MS-WIN-CRT-STDIO-L1-1-0.DLL
API-MS-WIN-CRT-STRING-L1-1-0.DLL
API-MS-WIN-CRT-TIME-L1-1-0.DLL
API-MS-WIN-CRT-UTILITY-L1-1-0.DLL
BCRYPT.DLL
CRYPT32.DLL
DNSAPI.DLL
KERNEL32.DLL
MSCOREE.DLL
MSVCP140.DLL
NCRYPT.DLL
NTDSAPI.DLL
OLE32.DLL
OLEAUT32.DLL
RPCRT4.DLL
SECUR32.DLL
SHLWAPI.DLL
USER32.DLL
VCRUNTIME140.DLL
VCRUNTIME140_1.DLL
VERSION.DLL
WEBSERVICES.DLL
WS2_32.DLL

*** 2) Platform API used per module ***

ADVAPI32.DLL
CloseServiceHandle
ControlService
OpenSCManagerA
OpenServiceA
QueryServiceStatus
RegisterServiceCtrlHandlerA
SetServiceStatus
StartServiceCtrlDispatcherA
StartServiceA
AddAccessAllowedAce
AddAccessDeniedAce
CreateWellKnownSid
InitializeAcl
InitializeSecurityDescriptor
SetSecurityDescriptorDacl
RegCloseKey
RegOpenKeyA
RegOpenKeyExA
RegQueryValueExA
GetUserNameA
OpenProcessToken
OpenThreadToken
GetTokenInformation
LookupAccountSidA
GetSidSubAuthority
GetSidSubAuthorityCount
DeregisterEventSource
RegisterEventSourceW
ReportEventW
RegisterEventSourceA
ReportEventA
ChangeServiceConfigA
QueryServiceConfigA
RegEnumKeyExA
GetLengthSid
ConvertStringSidToSidA
ConvertStringSidToSidA
API-MS-WIN-CRT-COMIO-L1-1-0.DLL
__getch

API-MS-WIN-CRT-CONVERT-L1-1-0.DLL
atoi
__atoi64
atol
strtol
strtoul
__i64toa
__itoa
__i64toa_s
atof
__ultoa
strtod
__ltoa
wcsombs
__strtod_l
__atoi64
atoi
strtoul

API-MS-WIN-CRT-ENVIRONMENT-L1-1-0.DLL
getenv
gconv

API-MS-WIN-CRT-FILESYSTEM-L1-1-0.DLL
remove
rename
__stat64i32
rename

API-MS-WIN-CRT-HEAP-L1-1-0.DLL
free
malloc
calloc
__get_heap_handle
realloc
__callnewh
__aligned_free
__aligned_malloc
free
free
free
malloc
__callnewh

API-MS-WIN-CRT-LOCALE-L1-1-0.DLL
setlocale
localeconv
__configthreadlocale
__create_locale
__free_locale
__configthreadlocale

API-MS-WIN-CRT-MATH-L1-1-0.DLL
ceilf
log
__fdopen
__setusermatherr
fabs
fmod
pow
ceil
floor
asin
atan
atan2
cos
sin
sqrt
tan
ceilf
log
__setusermatherr
fabs
fmod
pow
asin
atan
atan2
cos
sin
sqrt
tan

API-MS-WIN-CRT-RUNTIME-L1-1-0.DLL

signal

__invalid_parameter_noinfo_noreturn

_errno

raise

__invalid_parameter_noinfo

perror

exit

__beginthreadex

_strerror

system

__exit

abort

__ seh_filter_exe

_set_app_type

__configure_narrow_argv

__initialize_narrow_environment

__get_initial_narrow_environment

__initterm

__initterm_e

__p___argc

__p___argv

_cexit

_c_exit

_register_thread_local_exe_atexit_callback

_initialize_onexit_table
_register_onexit_function
_crt_atexit
terminate
__getpid
__wassert
raise
exit
__exit
__seh_filter_exe
__set_app_type
__configure_narrow_argv
__initialize_narrow_environment
__get_initial_narrow_environment
__initterm
__initterm_e
__p___argc
__p___argv
__register_thread_local_exe_atexit_callback
__initialize_onexit_table
__register_onexit_table
__crt_atexit

API-MS-WIN-CRT-STDIO-L1-1-0.DLL
__acrt_iob_func
__stdio_common_vfprintf
__stdio_common_vsprintf
__stdio_common_vsscanf
__stdio_common_vscanf
fclose
fgetpos
fopen
fsetpos
__get_osfhandle
__filelengthi64
feof
fflush
fgets
fputs
fseek
ftell
__stdio_common_vsnprintf_s
fwrite
setvbuf
fread
ferror
__stdio_common_vsprintf_s
__get_stream_buffer_pointers
fgetc
fputc
__fseeki64
ungetc
putc
__wfopen
__fileno
__setmode
__close
__lseek
_read
_write
__stdio_common_vswprintf
__set_fmode
__p__commode
_wsopen_dispatch
_filelengthi64
__stdio_common_vsprintf
__stdio_common_vswprintf
__stdio_common_vswprintf
__set_fmode
__p__commode

API-MS-WIN-CRT-STRING-L1-1-0.DLL
_strlwr
isdigit
isxdigit
tolower
strcspn
strncat
strncpy
strtok_s
__stricmp
strnlen
strspn
strtok
strcpy_s
strcat_s
_strdup
toupper
__strupr
__strncmp
isspace
isalnum
iscntrl
__wcsnicmp
isupper
strlen
strcpy
wcslen
strcat
__wcsupr
strtok_s
strcmp
strncpy
strlen
strcpy
strcat

API-MS-WIN-CRT-TIME-L1-1-0.DLL

_mktime64
__ftime64
__gmtime64
__localtime64
__time64
_difftime64
_time32
__timezone
clock
strftime
__daylight
_localtime32
__dstbias
__gmtime64_s
__tzname
_tzset
_tzset
_time64

API-MS-WIN-CRT-UTILITY-L1-1-0.DLL
qsort
bsearch

BCRYPT.DLL
BCryptGenRandom
BCryptGenRandom

CRYPT32.DLL
CertCreateCertificateContext
CertFreeCertificateContext
CertFreeCertificateChainEngine
CertGetCertificateChain
CertFreeCertificateChain
CertOpenStore
CertCloseStore
CertEnumCertificatesInStore
CertGetCertificateContextProperty
CryptProtectData
CryptUnprotectData
CryptProtectData
CryptUnprotectData

DNSAPI.DLL
DnsFlushResolverCacheEntry_A

KERNEL32.DLL
SetProcessShutdownParameters
FreeLibrary
GetProcAddress
LoadLibraryExA
SetConsoleCtrlHandler
GetLastError
 SetLastError
Sleep
CreateFileA
GetFileAttributesA
SetFileAttributesA
WriteFile
CloseHandle
SetCurrentDirectoryA
GetCurrentDirectoryA
CreateDirectoryA
DeleteFileA
FindClose
FindFirstFileA
FindNextFileA
GetDiskFreeSpaceA
GetDriveTypeA
GetFileSizeEx
LockFile
ReadFile
RemoveDirectoryA
SetEndOfFile
SetFilePointerEx
SetFileTime
UnlockFile
QueryPerformanceCounter
GetCurrentProcessId
GetCurrentThreadId
GlobalMemoryStatusEx
GetSystemInfo
GetWindowsDirectoryA
GetModuleFileNameA
GetModuleHandleA
GetLogicalDriveStringsA
GetTempPathA
CopyFileA
MoveFileA
MoveFileExA
CompareFileTime
QueryPerformanceFrequency
GetSystemTime
SystemTimeToFileTime
MultiByteToWideChar
WideCharToMultiByte
LocalAlloc
LocalFree
GetCurrentProcess
GetCurrentThread
ConnectNamedPipe
DisconnectNamedPipe
SetNamedPipeHandleState
CreateNamedPipeA
SetEvent
CreateEventA
OpenEventA
MapViewOfFile
UnmapViewOfFile
CreateFileMappingA
OpenFileMappingA
SetThreadPriority
CreateMutexA
RtlCaptureContext
GetEnvironmentVariableA
SuspendThread
ResumeThread
GetThreadContext
GetVersionExA
ReadProcessMemory
GetProcessTimes
FileTimeToSystemTime
GetStdHandle
DuplicateHandle
InitializeCriticalSection
EnterCriticalSection
LeaveCriticalSection
TryEnterCriticalSection
DeleteCriticalSection
ResetEvent
ReleaseSemaphore
WaitForSingleObject
TerminateProcess
GetExitCodeProcess
TerminateThread
GetExitCodeThread
CreateProcessA
WaitForMultipleObjects
CreateSemaphoreA
GetEnvironmentStrings
FreeEnvironmentStringsA
HeapAlloc
HeapFree
GetProcessHeap
GetVersion
PostQueuedCompletionStatus
TlsAlloc
FormatMessageA
FormatMessageW
DeviceIoControl
LoadLibraryA
GetOverlappedResult
CreateIoCompletionPort
GetQueuedCompletionStatus
TlsGetValue
TlsSetValue
CreateFileW
GetFileAttributesW
SetFileAttributesW
GetFileType
GetModuleHandleW
RtlVirtualUnwind
GetSystemTimeAsFileTime
GetTickCount
LoadLibraryW
GlobalMemoryStatus
FindFirstFileW
FindNextFileW
GetFileSize
FlushConsoleInputBuffer
SetHandleInformation
CreatePipe
RtlLookupFunctionEntry
UnhandledExceptionFilter
SetUnhandledExceptionFilter
IsProcessorFeaturePresent
InitializeCriticalSectionAndSpinCount
WaitForSingleObjectEx
CreateEventW
IsDebuggerPresent
CreateDirectoryW
DeleteFileW
GetDiskFreeSpaceW
RemoveDirectoryW
GetWindowsDirectoryW
IstrcmpW
MoveFileW
MoveFileExW
GetACP
GetThreadLocale
GetLocaleInfoA
GetTimeZoneInformation
GetGeoInfoW
GetUserGeoID
GetLocaleInfoW
GetNumberFormatW
GetCurrencyFormatW
SystemTimeToTzSpecificLocalTime
GetDateFormatW
GetTimeFormatW
GetCurrentDirectoryW
GetFullPathNameW
GetFullPathNameA
SetFilePointer
IsValidCodePage
IsDBCSLeadByteEx
RaiseException
InitializeCriticalSectionEx
VirtualProtect
VirtualQuery
OutputDebugStringW
Sleep
CopyFileA
CreateDirectoryA
CloseHandle
SetEndOfFile
FindClose
FindFirstFileA
FindNextFileA
GetCurrentDirectoryA
SetCurrentDirectoryA
CompareFileTime
GetSystemTime
SystemTimeToFileTime
WideCharToMultiByte
CreateNamedPipeA
DisconnectNamedPipe
ReadFile
WriteFile
InitializeCriticalSection
CreateEventA
CreateSemaphoreA
DeleteCriticalSection
EnterCriticalSection
GetCurrentProcessId
GetCurrentThreadId
GetExitCodeThread
LeaveCriticalSection
ReleaseSemaphore
ResetEvent
SetEvent
TerminateThread
TryEnterCriticalSection
FreeEnvironmentStringsA
GetEnvironmentStrings
GetEnvironmentVariableA
LeaveCriticalSection
FreeLibrary
GetProcAddress
LoadLibraryA
GetLastError
GetTempPathA
LocalFree
InitializeCriticalSectionEx

MSCOREE.DLL
_CorExeMain

MSVCP140.DLL
CyberArk

_Strcoll

_Strxfrm

_Xtime_get_ticks

_Mtx_init_in_situ

_Mtx_destroy_in_situ

_Mtx_lock

_Mtx_unlock

_Query_perf_counter

_Query_perf_frequency

_Strcoll

_Strxfrm

_Xtime_get_ticks

_Mtx_init_in_situ

_Mtx_destroy_in_situ

_Mtx_lock

_Mtx_unlock

_Query_perf_counter

_Query_perf_frequency

_Xlength_error

uncaught_exception

_Xbad_alloc

_Xout_of_range

_Xregex_error

_Throw_C_error

_Xbad_function_call

_Xinvalid_argument

_Fiopen

setw
_Syserror_map
_Xbad_alloc
_Xregex_error
_Throw_C_error
_Xbad_function_call
_Xinvalid_argument
_Fiopen
setw
_Syserror_map
_Getcvt
_Locinfo
~_Locinfo
_Getfalse
_Gettrue
_Getcoll
_Getconv
_Lockit
~_Lockit
operator=
~basic_ios<charCOMMABREAKstruct_std::char_traits<char>_>
setstate
widen
basic_ios<charCOMMABREAKstruct_std::char_traits<char>_>
clear
imbue
basic_iostream<charCOMMABREAKstruct_std::char_traits<char>_>
~basic_iostream<charCOMMABREAKstruct_std::char_traits<char>_>
basic_istream<charCOMMABREAKstruct_std::char_traits<char>_>
~basic_istream<charCOMMABREAKstruct_std::char_traits<char>\_>

_ipfx
operator>>&
operator>>&
get
operator>>&
seekg
tellg
read
basic_ostream<charCOMMABREAKstruct_std::char_traits<char>\_>
~basic_ostream<charCOMMABREAKstruct_std::char_traits<char>\_>
_Osfx
operator<<
operator<<
operator<<
operator<<
put
flush
write
`vbase_destructor`
operator<<
operator<<
operator<<
operator<<
operator<<
basic_streambuf<charCOMMABREAKstruct_std::char_traits<char>\_>
~basic_streambuf<charCOMMABREAKstruct_std::char_traits<char>\_>
sbumpc
sgetc
sputc
sputn
_Pninc
_Lock
_Unlock
imbue
setbuf
showmanyc
sync
uflow
xsgetn
xsputn
getloc
snextc
_Init
pbase
eback
gptr
pptr
egptr
epptr
_Lock
_Unlock
imbue
setbuf
showmanyc
sync
uflow
xsgetn
xsputn
always_noconv
in
out
unshift
_Getcat
~codecvt<unsigned_short<char>struct__Mbstatet>
codecvt<unsigned_short<char>struct__Mbstatet>
out
toupper
_Getcat
tolower
tolower
widen
narrow
exceptions
getloc
classic
_Init
_Getgloballocale
classic
_Init
_Getgloballocale
_New_Locimp
_Addfac
facet
~facet
Decref
_Incref
-Decref
_Incref
operator unsigned int64

NCRYPT.DLL
NCryptOpenStorageProvider
NCryptOpenKey
NCryptGetProperty
NCryptExportKey
NCryptFreeObject
NCryptOpenStorageProvider
NCryptOpenKey
NCryptGetProperty
NCryptExportKey
NCryptFreeObject

NTDSAPI.DLL
DsFreePasswordCredentials
DsMakePasswordCredentialsW

OLE32.DLL
IIDFromString
CoUninitialize
CoInitializeEx
CoCreateInstance
OLEAUT32.DLL
SysAllocStringLen
SysFreeString
VariantInit
VariantClear
VariantChangeType
VariantClear

RPCRT4.DLL
RpcStringFreeA
UuidCreate
UuidToStringA
RpcBindingSetOption
RpcBindingFromStringBindingW
RpcStringBindingComposeW
RpcBindingSetAuthInfoExW
RpcStringFreeW
RpcBindingFree
I_RpcBindingInqSecurityContext
NdrClientCall2

SECUR32.DLL
FreeContextBuffer
QueryContextAttributesW

SHLWAPI.DLL
PathFileExistsA
PathFindExtensionA
PathFindFileNameA
PathIsDirectoryA
PathMatchSpecA
PathRemoveFileSpecA
PathStripToRootA
PathFileExistsW
PathIsDirectoryW
PathRemoveFileSpecW
UrlUnescapeW
StrCmpW
StrCmpW
PathIsDirectoryA
PathFileExistsA
PathFindExtensionA
PathFindFileNameA
PathMatchSpecA
PathRemoveFileSpecA
PathStripToRootA

USER32.DLL
CharLowerA
CharUpperA
GetProcessWindowStation
GetUserObjectInformationW
MessageBoxW
GetDesktopWindow

VCRUNTIME140.DLL
memset
longjmp
__std_exception_copy
__std_exception_destroy
_CxxThrowException
memcpy
memmove
strchr
strstr
__purecall
__C_specific_handler
__std_type_info_name
memchr
memcmp
strchr
__std_type_info_compare
__std_type_info_hash
__RTDynamicCast
wcsstr
__intrinsic_setjmp
__current_exception
__current_exception_context
__RTtypeid
__FrameUnwindFilter
memset
longjmp
memcpy
strchr
strstr
__purecall
__C_specific_handler
__std_type_info_name
memchr
memcmp
strrchr
__std_type_info_compare
__std_type_info_hash
wcsstr
__intrinsic_setjmp
__RTtypeid

VCRUNTIME140_1.DLL
__CxxFrameHandler4
__CxxFrameHandler4

VERSION.DLL
GetFileVersionInfoSizeA
GetFileVersionInfoA
VerQueryValueA
GetFileVersionInfoSizeA
GetFileVersionInfoA
VerQueryValueA

WEBSERVICES.DLL
WsCreateError
WsGetErrorString
WsFreeError
WsCreateHeap
WsFreeHeap
WsOpenServiceProxy
WsCloseServiceProxy
WsFreeServiceProxy
WsCall
WsCreateServiceProxyFromTemplate
WsCreateError
WsGetErrorString
WsFreeError
WsCreateHeap
WsFreeHeap
WsOpenServiceProxy
WsCloseServiceProxy
WsFreeServiceProxy
WsCall
WsCreateServiceProxyFromTemplate

WS2_32.DLL
getaddrinfo
freeaddrinfo
inet_pton
inet_ntop
accept
bind
closesocket
connect
getpeername
getsockname
getsockopt
htonl
htons
ioctlsocket
inet_addr
inet_ntoa
listen
ntohl
ntohs
recv
recvfrom
select
send
sendto
setsockopt
shutdown
socket
gethostbyname
gethostname
WSAGetLastError
WSASetLastError
WSAStartup
WSACleanup
__WSAFDIsSet
__WSAFDIsSet
inet_addr
inet_ntop
9 Appendix B

c:\Program Files (x86)\PrivateArk\Server\libcrypto-1_1-x64.dll
c:\Program Files (x86)\PrivateArk\Server\libcurl.dll
c:\Program Files (x86)\PrivateArk\Server\libmysql.dll
c:\Program Files (x86)\PrivateArk\Server\libprotobuf-lite.dll
c:\Program Files (x86)\PrivateArk\Server\libprotobuf.dll
c:\Program Files (x86)\PrivateArk\Server\libsasl.dll
c:\Program Files (x86)\PrivateArk\Server\libssl-1_1-x64.dll
c:\Program Files (x86)\PrivateArk\Server\PARENEAgent.dll
c:\Program Files (x86)\PrivateArk\Server\PARNotificator.dll
c:\Program Files (x86)\PrivateArk\Server\PARVaultAgent.dll
c:\Program Files (x86)\PrivateArk\Server\RacControllerSDK.dll
c:\Program Files (x86)\PrivateArk\Server\ssleay32.dll
c:\Program Files (x86)\PrivateArk\Server\xalan-C_1_12_x64.dll
c:\Program Files (x86)\PrivateArk\Server\XalanMessages_1_12_x64.dll
c:\Program Files (x86)\PrivateArk\Server\xerces-c_3_2_2_x64.dll
c:\Program Files (x86)\PrivateArk\Server\Database\Bin\libcrypto-1_1-x64.dll
c:\Program Files (x86)\PrivateArk\Server\Database\Bin\libcurl.dll
c:\Program Files (x86)\PrivateArk\Server\Database\Bin\libprotobuf-lite.dll
c:\Program Files (x86)\PrivateArk\Server\Database\Bin\libprotobuf.dll
c:\Program Files (x86)\PrivateArk\Server\Database\Bin\libsasl.dll
c:\Program Files (x86)\PrivateArk\Server\Database\Bin\libssl-1_1-x64.dll
c:\Program Files (x86)\PrivateArk\Server\Database\MySQL Utilities\msvcp120.dll
c:\Program Files (x86)\PrivateArk\Server\Database\MySQL Utilities\msvcr120.dll
c:\Program Files (x86)\PrivateArk\Server\Database\MySQL Utilities\python27.dll
c:\Program Files (x86)\PrivateArk\Server\Event Notification Engine\libeay32.dll
c:\Program Files (x86)\PrivateArk\Server\Event Notification Engine\ssleay32.dll
c:\Program Files (x86)\PrivateArk\Server\LogicContainer\CyberArk.AppServices.Jwt.dll
c:\Program Files (x86)\PrivateArk\Server\LogicContainer\CyberArk.AppServices.LogicContainer.dll
c:\Program Files (x86)\PrivateArk\Server\LogicContainer\CyberArk.Casos.dll
c:\Program Files (x86)\PrivateArk\Server\LogicContainer\CyberArk.Infra.Logger.dll
c:\Program Files (x86)\PrivateArk\Server\LogicContainer\CyberArk.Services.Exceptions.dll
c:\Program Files (x86)\PrivateArk\Server\LogicContainer\log4net.dll
c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PowerCollections.dll
c:\Program Files (x86)\PrivateArk\Server\LogicContainer\BLDlls\Cyberark.DNA.Shared.Models.dll
c:\Program Files (x86)\PrivateArk\Server\LogicContainer\BLDls\Cyberark.DNA.Shared.ModelsContract.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\BLDls\Cyberark.LogicContainer.Shared.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\BLDls\FluentNHibernate.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\BLDls\lesi.Collections.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\BLDls\Microsoft.IdentityModel.Logging.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\BLDls\Microsoft.IdentityModel.Tokens.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\BLDls\MySQL.Data.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\BLDls\Newtonsoft.Json.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\BLDls\NHibernate.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\BLDls\NHibernate.XmlSerializers.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\BLDls\PIMSuiteBL.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\BLDls\PIMSuiteData.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\BLDls\System.IdentityModel.Tokens.Jwt.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\BLDls\WorkFlowManager.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\BouncyCastle.Crypto.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\Castle.Core.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\Castle.Windsor.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Data.Entities.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Data.Messaging.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Data.Messaging.Policies.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Infra.Base.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Infra.Common.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Infra.Engine.Contracts.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Infra.Engine.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Server.Adapters.PIM.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Server.Data.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Server.Engine.Contracts.Adapters.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Server.Engine.Contracts.App.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Server.Engine.Contracts.Packages.dll

Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Server.Engine.dll